Notice of Allowability	Application No.	Applicant(s)	
	09/747,238	GRAWROCK, DAVID W.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *examiner's amendment authorized on 12/20/06*.

2. ☒ The allowed claim(s) is/are *9 and 12-14*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William Schaal on 12/20/06.

The application has been amended as follows:

9. (Currently Amended) A method comprising:

transmitting a first command from a second device being an input/output control hub (ICH) to a first device being a trusted platform module (TPM);

generating a long term value within the first device, the long term value generated upon detecting an initial power-up sequence and receipt of information from the second device;

permanently storing the long term value within a protected area of an internal memory of the first device;

providing the long term value to the second device communicatively coupled to the first device;

generating a short term value within the first device, the short term value is modified after each power cycle;

providing the short term value to the second device;

generating a secret value within the first device after each power cycle, the secret value being a combination of both the long term value and the short term value; ~~and~~

generating the secret value within the second device based on the long term value and the short term value; and

using the secret value to encrypt and decrypt data transmitted between the first device and the second device.

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method of generating a secret value shared between a first device and a second device. More specifically, independent claim 1 identifies the uniquely distinct features: generating a long term value within the first device, the long term value generated upon detecting an initial power-up sequence and receipt of information from the second device; providing the long term value to the second device; generating a short term value within the first device; providing the short term value to the second device; generating a secret value within the first device and the second device, the secret value being a combination of both the long term value and the short term value; the first device being a trusted platform module (TPM) and the second device being an input/output control hub (ICH). The closest prior art include: (i) Davis (5,818,939) for disclosing a method in which a chipset communicates with a cryptographic unit when both devices are powered up during manufacture, the cryptographic unit then generates a shared secret key which is a long-term value, and stores the long-term shared key in a protected internal memory (fig. 4; col. 5, lines 25-44); (ii) Menezes ("Handbook of Applied

Cryptography") for disclosing a method for generating a shared session key that is a combination of a shared long-term value, and a short-term value (p. 499, 2nd paragraph); (iii) Levy et al (6,212,633) for disclosing a method for generating a new session key in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62); and (iv) Burns ("INTEL: Intel introduces new chipset for intel Pentium III processor-based performance PCs") for disclosing an input/output control hub (ICH) . However, Davis, Menezes, Levy, and Burns, either alone or in combination, do not teach the specific features mentioned above. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

KAMBIZ ZAND
PRIMARY EXAMINER

Minh Dinh
Examiner
Art Unit 2132

MD
12/20/06